Upgrade Instructions: Web Security Gateway

Upgrade Instructions | Web Security Gateway | Version 7.8.x

These instructions describe how to upgrade Websense Web Security Gateway server components (Windows, Linux, or appliance) from **v7.7.x** to **v7.8.x**.

> **Important**
>
> Because Content Gateway and Websense appliances must be at v7.7.x to upgrade to v7.8.x, it is not possible to upgrade directly from v7.6.x to v7.8.x.
>
> If you are currently running a Web Security Gateway version earlier than v7.7.x, upgrade to v7.7.x first, then upgrade to v7.8.x. See Upgrading Websense Web Security Solutions to v7.7 for instructions.

Note that the following operating systems are no longer supported in v7.8.x. If you are using one of these operating systems, you must migrate your operating system before upgrading to v7.8.x, as outlined below:

Red Hat Enterprise Linux 5	1. Migrate to Red Hat Enterprise Linux 6. 2. Upgrade to v7.8.x on the new platform.
Windows 2008 (32-bit)	1. Migrate to Windows 2008 R2. 2. Upgrade to v7.8.x on the new platform.

To perform a migration and upgrade, see Order of migration and upgrade steps for v7.8.x (find links to detailed instructions at the bottom of the page, under the table).

The upgrade process is designed for a properly functioning Websense Web Security Gateway deployment. Upgrading does not repair a non-functional system.

Beginning with v7.8.4, you have the option to upgrade your Web Security deployment incrementally, rather than upgrading all machines and components at the same time. This allows you to upgrade individual Policy Server instances and their dependent components as separate "logical deployments." Policy Server instances that have not

been upgraded and their dependent components continue to function normally at v7.8.3. Please see the new Incremental Upgrade guide for details.

> **Important**
>
> Before you start the upgrade process, the SQL Server Agent jobs associated with the Log Database must be stopped as described in *Step 1: Prepare for upgrade*, page 2. Please coordinate with your database administrator, if needed, before beginning the upgrade process.
>
> Note that this requirement does not apply to SQL Server Express.

- *Step 1: Prepare for upgrade*, page 2
- *Step 2: Prepare appliances for upgrade (appliance-only)*, page 4
- *Step 3: Prepare to upgrade Content Gateway*, page 6
- *Step 4: Restart services before starting the upgrade*, page 8
- *Step 5: Upgrade the Policy Broker machine*, page 9
- *Step 6: Upgrade additional Policy Server machines*, page 13
- *Step 7: Upgrade additional Filtering Service, Network Agent, and User Service machines*, page 18
- *Step 8: Upgrade Websense Log Server*, page 22
- *Step 9: Upgrade the TRITON management server*, page 23
- *Step 10: Upgrade software instances of Content Gateway*, page 25
- *Step 11: Upgrade any additional components*, page 39

Step 1: Prepare for upgrade

Before upgrading Web Security Gateway:

1. Make sure the installation machine meets the hardware and operating system recommendations in System requirements for this version.
2. Verify that third-party components that work with Web Security Gateway, including your database engine and directory service, are supported. See Requirements for Web Security solutions.
3. Back up all of your Websense components before starting the upgrade process. See the Backup and Restore FAQ for instructions.

   The Backup and Restore FAQ includes instructions for backing up all of the pieces that make up Web Security Gateway on all platforms:

   - TRITON Infrastructure
   - Web Security components
   - Content Gateway

On Websense appliances, be sure to perform a **full appliance configuration** backup.

4. Before upgrading Websense Filtering Service, make sure that the Filtering Service machine and the TRITON management server have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.

5. Back up your current Log Database and stop Log Server.

   Warning

   If database operations are active during upgrade, the Websense Log Database may be left in an inconsistent state, rendering it unusable.

   When this occurs, it can be difficult to fix.

   Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

   a. Back up Web Security reporting databases.

      Refer to Microsoft documentation for instructions on backing up databases. The Websense Web Security databases are named wslogdb70 (the catalog database), wslogdb70_*n* (standard logging partition databases), and wslogdb70_amt_1 (threats partition database).

   b. On the Log Server machine, use the Windows Services tool to stop **Websense Log Server**.

6. Stop all database jobs associated with the Web Security Log Database:

   If you have a **full version of Microsoft SQL Server** (not Express):

   a. Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).

   b. To disable all currently active Websense SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:

      - Websense_ETL_Job_wslogdb70
      - Websense_AMT_ETL_wslogdb70
      - Websense_IBT_DRIVER_wslogdb70
      - Websense_Trend_DRIVER_wslogdb70
      - Websense_Maintenance_Job_wslogdb70

      Disabling the jobs prevents them from executing at the next scheduled time, but does not stop them if a job is in process.

      Make sure all jobs have completed any current operation before proceeding with upgrade.

   c. After upgrade, remember to enable the disabled jobs to resume normal database operations.

If you have **SQL Server Express**, use the Windows Services tool to restart the MSSQLSERVER service prior to upgrade, in order to ensure that the Service Broker jobs are not running.

7. If Websense Log Server uses a Windows trusted connection to access the Log Database, be sure to log on to the Log Server machine using the trusted account to perform the upgrade. To find out which account is used by Log Server:
   a. Launch the Windows Services tool.
   b. Scroll down to find **Websense Log Server**, then check the **Log On As** column to find the account to use.
8. If your deployment includes V-Series appliances, continue with the next section (*Step 2: Prepare appliances for upgrade (appliance-only)*, page 4.

   If you have a software-only deployment, skip to *Step 4: Restart services before starting the upgrade*, page 8.

Step 2: Prepare appliances for upgrade (appliance-only)

Before applying the 7.8.x patch, perform the following tasks and be aware of the following issues.

Apply the v7.7 pre-upgrade hotfix

Before upgrading any Websense appliance to v7.8.x, a v7.7.x hotfix is required.

Until the hotfix is installed, it is not possible to download (or upload) the v7.8.x upgrade patch files to the appliance.

1. To get the hotfix, in the Appliance manager, go to the **Hotfixes** tab of the **Administration** > **Patches/ Hotfixes** page.
2. Enter the name of the hotfix to download and install on the appliance if it's not in the drop-down list. For example, if you are upgrading from:
   - v7.7.0, look for APP-7.7.0-090
   - v7.7.3, look for APP-7.7.3-090
3. Click **Find** to locate the hotfix.
4. Click **Download**.

   When the download is done, the hotfix appears in the table of downloaded hotfixes with the status **Ready to install**.
5. Click **Install** to apply the hotfix. The installation may temporarily interrupt some services.
6. Click **OK** to continue. It may take more than 5 minutes to install the hotfix.

After the hotfix is installed, manually restart the appliance from the Appliance manager:

1. Navigate to the **Status** > **General** page.

2. Under Appliance Controller, click **Restart Appliance**.

   Restarting the appliance takes from 5 to 8 minutes. The appliance has successfully restarted when you're returned to the Appliance manager logon page.

Repeat this process for each appliance that you intend to upgrade to v7.8.x.

Note that each appliance must be upgraded to v7.8.1 before upgrading to v7.8.2.

Content Gateway hotfix

Content Gateway upgrades from v7.7.x to v7.8.x require an additional step to avoid possible latency issues sometimes caused by scanning using async mode.

1. Versions older than v7.7.x should first upgrade to v7.7.x.
2. Download and install v7.7.x Hotfix 94. This hotfix adds background variables that retain sync mode.
3. Upgrade from v7.7.x to v7.8.x. Sync mode is retained.

Content Gateway logs

During the upgrade, depending on their size, older Content Gateway logs may be automatically removed. If you want to retain all Content Gateway logs, you can download the Content Gateway logging directory before starting the upgrade.

1. In the Appliance Manager, go to **Administration > Logs**.
2. Select the **Websense Content Gateway** module and then **Download entire log file**.
3. Click **Submit** and specify a location to save the file.

Policy databases and Websense databases are not affected by the upgrade.

Network Agent settings

In the majority of deployments, upgrade preserves all Network Agent settings.

However, when the following conditions are true, the upgrade process does not preserve several Network Agent settings:

- There is a Filtering only appliance that is configured to get policy information from the Policy Broker machine (either the Full policy source appliance or an off-appliance software installation).
- There is an off-appliance Network Agent installation that uses the Filtering Service on the Filtering only appliance, and uses the Policy Server on the Policy Broker machine.

When the above conditions are true and the upgrade is performed, the settings for the off-appliance Network Agent installation are not retained.

In this case, record your Network Agent settings (configured in the Web Security manager) before performing the upgrade. Go to the Local Settings page for each Network Agent instance (**Settings > Network Agent** > *agent_IP_address*) and record **all** of its settings.

The following local settings are not preserved.

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

NIC Configuration settings (from the **Settings > Network Agent > NIC Configuration** page for each NIC) are also not preserved:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

Save your record where you can easily access it when the upgrade is complete.

Disable on-appliance TRITON console

In version 7.8.x, the Web Security manager cannot reside on an appliance. Disable the on-appliance TRITON console and create a Windows-based TRITON management server before upgrading.

Complete instructions can be found in Migrating the Web Security manager off of a Websense appliance.

Step 3: Prepare to upgrade Content Gateway

There are several large and important changes beginning in version 7.8.2. Please read the 7.8.3Release Notes before starting the upgrade.

SSL support

SSL support is rearchitected in version 7.8. Most SSL configuration settings are saved and applied to the upgraded Content Gateway.

During upgrade:

- The v7.7.x SSL SQLite3 database is converted to a new database file.
- The Incident list is retained.
- Dynamic certificates are not retained. All other certificates are retained.

- The Certificate Authority Tree is retained (trusted Root CA tree).
- SSLv2 is no longer enabled by default. If it is enabled prior to upgrade, the setting is retained.
- CRL and OCSP revocation statistics (on Monitor > SSL > CRL Statistics) are retained.
- Customized certificate failure and connect error message pages are not retained.
- SSL **inbound*.log** and **outbound*.log** files are deleted. After upgrade, transaction logging is sent to **extended.log** or **squid.log** when the logging subsystem is configured for "Log Transactions and Errors" or "Log Transactions Only". Otherwise, logging is sent to **content_gateway.out**.

Before upgrading:

- Content Gateway upgrades from v7.7.x to v7.8.x require an additional step to avoid possible latency issues sometimes caused by scanning using async mode.
  1. Versions older than v7.7.x should first upgrade to v7.7.x.
  2. Download and install v7.7.x Hotfix 94. This hotfix adds background variables that retain sync mode.
  3. Upgrade from v7.7.x to v7.8.x. Sync mode is retained.
- Consider performing maintenance on the Incident list; remove unwanted entries.
- Note customizations to certificate failure and connect error message pages. The code structure of the pages has changed; you cannot simply reapply (paste) the 7.7.x HTML.

User authentication

The upgrade process converts existing Multiple Realm Authentication rules into equivalent Rule-Based Authentication rules, with some important changes in structure.

Consolidated credential caching

There is one credential cache for both explicit and transparent proxy mode, and one Global Authentication Options page for setting the caching method and Time-To-Live.

During upgrade:

- (For upgrades from 7.7.x to 7.8.x) The credential cache Enabled/Disabled setting for explicit proxy is retained from the Global Authentication Options tab. Caching for transparent proxy traffic is always enabled.
- The Authentication Mode setting (IP address or Cookie mode) is retained from the Transparent Proxy Authentication tab.
- The Cache TTL value is retained from Transparent Proxy Authentication tab unless the value on the Global Authentication Options tab is not the default, in which case the customized value is used. The cache TTL value is in minutes.

- IP addresses and ranges on the Global Authentication Options Multi-user IP Exclusions list are moved to the cookie cache IP address list.
- If cookie caching is enabled in a Multiple Realm rule, the source IP addresses from that rule are copied to cookie cache IP address list.

Integrated Windows Authentication (IWA)

After upgrade, always check and, if necessary, rejoin IWA domains.

- Upgrade to version 7.8.1 should preserve exiting IWA domain joins.
- Upgrade to version 7.8.2 breaks IWA domain joins. Therefore, IWA domains must be rejoined.

Important

If your deployment uses IWA and a load balancer:

- Version 7.8.1 does not support the configuration.
- Versions 7.8.2 and 7.8.3 support load balancers, however, post-upgrade a special configuration must be applied. Follow the configuration steps described in the v7.8.2 Release Notes or the v7.8.3 Release Notes.

Features to configure after upgrade

You may want to review and configure the following enhanced features post-upgrade.

- Range-based IP spoofing. If you use IP spoofing, see the Help system for information about how range-based IP spoofing can address a boarder range of source IP address requirements when traffic is routed through Content Gateway.
- WCCP configuration synchronization in a cluster. It's now possible to disable WCCP configuration synchronization.

Step 4: Restart services before starting the upgrade

Most Websense services must be running before the upgrade process begins. If any service (other than Log Server) is stopped, start it before initiating the upgrade.

The installer will stop and start Websense services as part of the upgrade process. If the services have been running uninterrupted for several months, the installer may not be able to stop them before the upgrade process times out.

- To ensure the success of the upgrade, manually stop and start all the Websense services **except Log Server** before beginning the upgrade. (Log Server should remain stopped, as described in *Step 1: Prepare for upgrade*, page 2.)
  - *Windows*: Navigate to the Websense **Web Security** directory (C:\Program Files (x86)\Websense\Web Security\, by default) and enter the following command:

```
WebsenseAdmin restart
```

- *Linux*: Navigate to the **Websense** directory (/opt/Websense/, by default) and enter the following command:

  ```
  ./WebsenseAdmin restart
  ```

- On Windows machines, if you have configured the **Recovery** properties of any Websense service to restart the service on failure, use the Windows Services dialog box to change this setting to **Take No Action** before upgrading.

Internet access during the upgrade process

When you upgrade, policy enforcement stops when Websense services are stopped. Users have unrestricted access to the Internet until the Websense services are restarted.

The Websense Master Database is removed during the upgrade process. Websense Filtering Service downloads a new Master Database after the upgrade is completed.

Step 5: Upgrade the Policy Broker machine

You must upgrade the machine that hosts the primary (or standalone) **Websense Policy Broker** first, regardless of which other components on are on the machine. Policy Broker may reside on:

- A Websense **full policy source** appliance
- A Windows Server 2008 R2 or R2 SP1, or 2012 (64-bit) machine
- A RHEL 6.x machine (64-bit)

Any other components on the Policy Broker machine are upgraded along with Policy Broker.

If your configuration includes a primary Policy Broker and one or more replica Policy Brokers, you must upgrade the primary Policy Broker first. An attempt to upgrade a replica Policy Broker without first upgrading the primary will result in an error message. You will be required to exit the upgrade for that machine and upgrade the primary Policy Broker before continuing.

Upgrade replica Policy Brokers after the primary has been upgraded and before attempting to upgrade any Policy Servers associated with them. If Policy Server is installed on the same machine, it will be upgraded at the same time.

Jump to the section with the upgrade instructions for the platform that hosts the primary (or standalone) Policy Broker:

- *Policy Broker: Appliance upgrade instructions*, page 10
- *Policy Broker: Windows upgrade instructions*, page 11
- *Policy Broker: Linux upgrade instructions*, page 12

Policy Broker: Appliance upgrade instructions

Before you begin:

- Make sure you have finished installing Hotfix 90, as described in the preparation steps at the start of the upgrade instructions.
- Log on to the Appliance manager directly, rather than using single sign-on from the TRITON console. This avoids potential timeout problems while the upgrade patch is being loaded onto the appliance.
- Take all precautions to ensure that power to the V-Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.

1. To download the upgrade patch, in the Appliance manager, go to the **Administration > Patches/Hotfixes > Patches** page.

   If the 7.8.1 upgrade patch is not listed in the table of **Available patches**, click **Check for Patches**.

   - If a security warning appears, click **Continue**, mark the **I accept the risk...** check box, and then click **Run**.
   - The v7.8.1 upgrade patch includes 2 files: an **rpm** file and an **img** file.

     If you copy the patch from one appliance to other appliances, select **both files** at the same time in the Upload Patch utility. If you try to upload one file, then the other, a warning message is displayed, and the upload cannot be completed successfully.

2. Click **Download**. The combined size of the patch files is over 6 GB, so the process may take some time.

   When the download is done, the patch status becomes **Ready to Install**.

3. Click **Install** to apply the patch.
4. A **system check** is launched to verify that your system is ready for upgrade. This may take several minutes.
5. After the check succeeds, if you skipped the preparation step of backing up your files, click **Back Up**. If you are performing the backup now:

   a. Provide the connection information for the remote machine where the backup files will reside, then click **Test Connection**.

   b. Click **Run Backup Now**.

   Wait for the backup process to complete.

6. Click **Install Patch**.
7. Review the subscription agreement, then mark the **I accept this agreement** check box and click **Continue**.
8. A confirmation message tells you that during the upgrade, you are logged out of the Appliance manager and the appliance restarts twice. Click **OK** to begin the upgrade.

   The upgrade process may take up to 2 hours to complete.

9. After the appliance has automatically restarted twice, log on to the Appliance manager.

10. Navigate to the **Administration** > **Patches/Hotfixes** > **Patches** page.
11. Under **Patch History**, for version 7.8.1, verify that an **Upgrade Succeeded** status appears in the Comments section.
12. Navigate to the **Configuration** > **System** page and confirm the **Time and Date** settings, paying particular attention to the time zone setting. Make adjustments if needed.

When the appliance upgrade is complete, continue with *Step 6: Upgrade additional Policy Server machines*.

Do not upgrade any other appliances or off-appliance components until the full policy source appliance has successfully completed the upgrade process.

To finish the upgrade process for the Content Gateway module on the appliance, be sure to perform the steps in *Step 12: Post-upgrade activities for Content Gateway*, page 42.

Policy Broker: Windows upgrade instructions

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

   Important
   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   Warning
   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON78xSetup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
5. Right-click **WebsenseTRITON78xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks whether you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized, then the **Installing Websense** screen appears.

    If Policy Broker resides on the TRITON management server, or with Log Server, the upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

    Important
    The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Policy Broker: Linux upgrade instructions

1. Make sure no administrators are logged on to the TRITON console.
2. Log on the installation machine with administrator privileges (typically, as **root**).
3. Close all applications and stop any antivirus software.
4. Check the **etc/hosts** file. If there is no host name for the machine, add one.
5. Create a setup directory for the installer files, such as **/root/Websense_setup**.
6. Download the Web Security Linux installer from the Downloads page at mywebsense.com. The installer file is called **WebsenseTRITON78xSetup.exe**.
7. Uncompress the installer file and use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

   To launch the command-line installer, omit the -g switch:

```
./install.sh
```

8. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

9. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
10. On the Websense Upgrade screen, select **Start the upgrade** and then click **Next**.
11. When you click **Next**, a "Stopping All Services" progress message appears. Wait for Websense services to be stopped.

    The Pre-Upgrade Summary screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually using the **/opt/Websense/WebsenseAdmin stop** command. You can leave the installer running when you do so. Once you have manually stopped the services, return to the installer.
12. On the Pre-Upgrade Summary screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
13. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
14. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

15. If you stopped your antivirus software, restart it.

Step 6: Upgrade additional Policy Server machines

The central Policy Server resides on the same machine as Policy Broker, and was automatically upgraded in the previous section.

If you have additional Policy Server instances, upgrade them next, regardless of what other services reside on the machines. Policy Server may reside on:

- A Websense **user directory and filtering** appliance
- A Windows Server 2008 R2 or R2 SP1, or 2012 (64-bit) machine

- A RHEL 6.x machine (64-bit)

Jump to the section with the upgrade instructions for the platform that hosts Policy Server:

- *Policy Server: Appliance upgrade instructions*, page 14
- *Policy Server: Windows upgrade instructions*, page 15
- *Policy Server: Linux upgrade instructions*, page 16

Policy Server: Appliance upgrade instructions

Before you begin:

- Make sure you have finished installing Hotfix 90, as described in the preparation steps at the start of the upgrade instructions.
- Log on to the Appliance manager directly, rather than using single sign-on from the TRITON console. This avoids potential timeout problems while the upgrade patch is being loaded onto the appliance.
- Take all precautions to ensure that power to the V-Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.

1. To download the upgrade patch, in the Appliance manager, go to the **Administration > Patches/Hotfixes > Patches** page.

   If the 7.8.1 upgrade patch is not listed in the table of **Available patches**, click **Check for Patches**.

   - If a security warning appears, click **Continue**, mark the **I accept the risk...** check box, and then click **Run**.
   - The v7.8.1 upgrade patch includes 2 files: an **rpm** file and an **img** file.

     If you copy the patch from one appliance to other appliances, select **both files** at the same time in the Upload Patch utility. If you try to upload one file, then the other, a warning message is displayed, and the upload cannot be completed successfully.

2. Click **Download**. The combined size of the patch files is over 6 GB, so the process may take some time.

   When the download is done, the patch status becomes **Ready to Install**.

3. Click **Install** to apply the patch.
4. A **system check** is launched to verify that your system is ready for upgrade. This may take several minutes.
5. After the check succeeds, if you skipped the preparation step of backing up your files, click **Back Up**. If you are performing the backup now:

   a. Provide the connection information for the remote machine where the backup files will reside, then click **Test Connection**.

   b. Click **Run Backup Now**.

   Wait for the backup process to complete.

6. Click **Install Patch**.

7. Review the subscription agreement, then mark the **I accept this agreement** check box and click **Continue**.
8. A confirmation message tells you that during the upgrade, you are logged out of the Appliance manager and the appliance restarts twice. Click **OK** to begin the upgrade.

   The upgrade process may take up to 2 hours to complete.
9. After the appliance has automatically restarted twice, log on to the Appliance manager.
10. Navigate to the **Administration** > **Patches/Hotfixes** > **Patches** page.
11. Under **Patch History**, for version 7.8.1, verify that an **Upgrade Succeeded** status appears in the Comments section.
12. Navigate to the **Configuration** > **System** page and confirm the **Time and Date** settings, paying particular attention to the time zone setting. Make adjustments if needed.

When the appliance upgrade is complete, continue with *Step 7: Upgrade additional Filtering Service, Network Agent, and User Service machines*.

Do not upgrade any other appliances or off-appliance components until the full policy source appliance has successfully completed the upgrade process.

To finish the upgrade process for the Content Gateway module on the appliance, be sure to perform the steps in *Step 12: Post-upgrade activities for Content Gateway*, page 42.

Policy Server: Windows upgrade instructions

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

   Important

   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   Warning

   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON78xSetup.exe**.

- Installer files occupy approximately 2 GB of disk space.

5. Right-click **WebsenseTRITON78xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

Important

The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Policy Server: Linux upgrade instructions

1. Make sure no administrators are logged on to the TRITON console.
2. Log on the installation machine with administrator privileges (typically, as **root**).
3. Close all applications and stop any antivirus software.
4. Check the **etc/hosts** file. If there is no host name for the machine, add one.
5. Create a setup directory for the installer files, such as **/root/Websense_setup**.

6. Download the Web Security Linux installer from the Downloads page at mywebsense.com. The installer file is called **WebsenseWeb78xSetup_Lnx.tar.gz**.
7. Uncompress the installer file and use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

   To launch the command-line installer, omit the -g switch:

   ```
   ./install.sh
   ```
8. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

9. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
10. On the Websense Upgrade screen, select **Start the upgrade** and then click **Next**.
11. When you click **Next**, a "Stopping All Services" progress message appears. Wait for Websense services to be stopped.

    The Pre-Upgrade Summary screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually using the **/opt/Websense/WebsenseAdmin stop** command. You can leave the installer running when you do so. Once you have manually stopped the services, return to the installer.
12. On the Pre-Upgrade Summary screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
13. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
14. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

15. If you stopped your antivirus software, restart it.

Step 7: Upgrade additional Filtering Service, Network Agent, and User Service machines

If you have additional Filtering Service, Network Agent, or User Service instances, upgrade them next, regardless of what other services reside on the machines. Filtering Service, Network Agent, and User Service may reside on:

- A Windows Server 2008 R2 or R2 SP1, or 2012 (64-bit) machine
- A RHEL 6.x machine (64-bit)

Filtering Service and Network Agent may also reside on Websense **filtering only** appliances.

Filtering Service and Network Agent: Appliance upgrade instructions

Before you begin:

- Make sure you have finished installing Hotfix 90, as described in the preparation steps at the start of the upgrade instructions.
- Log on to the Appliance manager directly, rather than using single sign-on from the TRITON console. This avoids potential timeout problems while the upgrade patch is being loaded onto the appliance.
- Take all precautions to ensure that power to the V-Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.

1. To download the upgrade patch, in the Appliance manager, go to the **Administration > Patches/Hotfixes > Patches** page.

   If the 7.8.1 upgrade patch is not listed in the table of **Available patches**, click **Check for Patches**.

   - If a security warning appears, click **Continue**, mark the **I accept the risk...** check box, and then click **Run**.
   - The v7.8.1 upgrade patch includes 2 files: an **rpm** file and an **img** file.

     If you copy the patch from one appliance to other appliances, select **both files** at the same time in the Upload Patch utility. If you try to upload one file, then the other, a warning message is displayed, and the upload cannot be completed successfully.

2. Click **Download**. The combined size of the patch files is over 6 GB, so the process may take some time.

   When the download is done, the patch status becomes **Ready to Install**.

3. Click **Install** to apply the patch.
4. A **system check** is launched to verify that your system is ready for upgrade. This may take several minutes.

5. After the check succeeds, if you skipped the preparation step of backing up your files, click **Back Up**. If you are performing the backup now:
   a. Provide the connection information for the remote machine where the backup files will reside, then click **Test Connection**.
   b. Click **Run Backup Now**.

   Wait for the backup process to complete.
6. Click **Install Patch**.
7. Review the subscription agreement, then mark the **I accept this agreement** check box and click **Continue**.
8. A confirmation message tells you that during the upgrade, you are logged out of the Appliance manager and the appliance restarts twice. Click **OK** to begin the upgrade.

   The upgrade process may take up to 2 hours to complete.
9. After the appliance has automatically restarted twice, log on to the Appliance manager.
10. Navigate to the **Administration** > **Patches/Hotfixes** > **Patches** page.
11. Under **Patch History**, for version 7.8.1, verify that an **Upgrade Succeeded** status appears in the Comments section.
12. Navigate to the **Configuration** > **System** page and confirm the **Time and Date** settings, paying particular attention to the time zone setting. Make adjustments if needed.

When the appliance upgrade is complete, continue with *Step 8: Upgrade Websense Log Server*.

Do not upgrade any other appliances or off-appliance components until the full policy source appliance has successfully completed the upgrade process.

To finish the upgrade process for the Content Gateway module on the appliance, be sure to perform the steps in *Step 12: Post-upgrade activities for Content Gateway*, page 42.

Filtering Service, Network Agent, or User Service: Windows upgrade instructions

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

> **Important**
> If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   Warning
   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON78xSetup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
5. Right-click **WebsenseTRITON78xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

    Important
    The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Filtering Service, Network Agent, or User Service: Linux upgrade instructions

1. Make sure no administrators are logged on to the TRITON console.
2. Log on the installation machine with administrator privileges (typically, as **root**).
3. Close all applications and stop any antivirus software.
4. Check the **etc/hosts** file. If there is no host name for the machine, add one.
5. Create a setup directory for the installer files, such as **/root/Websense_setup**.
6. Download the Web Security Linux installer from the Downloads page at mywebsense.com. The installer file is called **WebsenseWeb78xSetup_Lnx.tar.gz**.
7. Uncompress the installer file and use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

   To launch the command-line installer, omit the -g switch:

   ```
   ./install.sh
   ```
8. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

9. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
10. On the Websense Upgrade screen, select **Start the upgrade** and then click **Next**.
11. When you click **Next**, a "Stopping All Services" progress message appears. Wait for Websense services to be stopped.

    The Pre-Upgrade Summary screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually using the **/opt/Websense/WebsenseAdmin stop** command. You can leave the installer running when you do so. Once you have manually stopped the services, return to the installer.
12. On the Pre-Upgrade Summary screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
13. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.

14. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

15. If you stopped your antivirus software, restart it.

Step 8: Upgrade Websense Log Server

Next, upgrade the Websense Log Server machine. Any other services on the machine are also upgraded.

Log Server runs on Windows Server 2008 R2 or R2 SP1, or 2012 (64-bit) machines.

To upgrade Log Server:

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

> **Important**
> If Log Server uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

> **Warning**
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON78xSetup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
5. Right-click **WebsenseTRITON78xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.

    The upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.

    During an upgrade to v7.8.4, a new logging partition is added to your Log Database to accommodate the new IPv6 feature.
12. Reboot the machine.

Important

The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.
14. Enable the SQL Server Agent jobs that you disabled prior to upgrade.

Step 9: Upgrade the TRITON management server

If you have not already upgraded the TRITON management server in the course of upgrading another component, use the following steps to upgrade the management server machine.

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.
3. Close all applications and stop any antivirus software.

> **Warning**
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON78xSetup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
5. Right-click **WebsenseTRITON78xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.

    The upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Step 10: Upgrade software instances of Content Gateway

Content Gateway runs on Websense full policy source, user directory and filtering, and filtering only appliances (all of which should already have been upgraded at this point).

Content Gateway is also:

- **Certified** on Red Hat Enterprise Linux, updates 4 and 5
  - Kernel version for 6.5: 2.6.32-431 (not recommended for v7.8.3 Content Gateway)
  - Kernel version for 6.4: 2.6.32-358
- **Supported** on Red Hat Enterprise Linux and CentOS 6, updates 0, 1, 2, 3, 4, and 5
  - Kernel version for 6.3: 2.6.32-279
  - Kernel version for 6.2: 2.6.32-220
  - Kernel version for 6.1: 2.6.32-131
  - Kernel version for 6.0: 2.6.32-71

To display the kernel version installed on your system, enter the command:

```
/bin/uname -r
```

If you have software instances of Content Gateway, make sure the host system meets the following hardware requirements before upgrading:

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum 8 GB recommended
Disk Space	2 disks: • 100 GB for the operating system, Content Gateway, and temporary data. • Max 147 GB for caching If caching will not be used, this disk is not required. The caching disk: – Should be at least 2 GB and no more than 147 GB – Must be a raw disk, not a mounted file system – Must be dedicated – Must *not* be part of a software RAID – Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64 MB of write-through cache
Network Interfaces	2

In addition, to support **transparent proxy** deployments:

Router	Must support WCCP v2. A Cisco router must run IOS 12.2 or later. The latest version is recommended. Client machines, the destination Web server, and Content Gateway must reside on different subnets.
—or—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). Websense Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Next, choose your upgrade procedure:

- For Content Gateway v7.7.x hosted on Red Hat Enterprise Linux **6 series**, see the section "Content Gateway: RHEL 6 upgrade instructions" below.
- For Content Gateway v7.7.x hosted on Red Hat Enterprise Linux **5 series**, see the section "Content Gateway: Upgrade Red Hat Enterprise Linux 5-series to 6-series during the Content Gateway upgrade" below.

Content Gateway: RHEL 6 upgrade instructions

This section describes upgrading Content Gateway v7.7.x to v7.8.x on your pre-existing Red Hat Enterprise Linux 6 host. If you are also upgrading Red Hat Enterprise Linux 5 to Red Hat Enterprise Linux 6, see the section "Content Gateway:

Upgrade Red Hat Enterprise Linux 5-series to 6-series during the Content Gateway upgrade" below.

> **Important**
>
> At the beginning of the upgrade procedure, the installer checks to see if the partition that hosts **/opt** has enough space to hold a copy of the existing Content Gateway log files (copied to **/opt/WCG_tmp/logs**). If there's not enough space, the installer prints an error message and quits.
>
> In this situation, if you want to retain the log files you must copy the contents of **/opt/WCG/logs** to a location that has enough space, and then delete the log files in **/opt/WCG/logs**.
>
> When the upgrade is complete, move the files from the temporary location back to **/opt/WCG/logs** and delete the files in the temporary location.

> **Note**
>
> If you have multiple Content Gateway instances deployed in a cluster, you **do not** have to disable clustering or VIP (if used). As each member of the cluster is upgraded it will rejoin the cluster.

1. If your Web Security Gateway solution is deployed with Data Security, log on to the Content Gateway manager and go to the **Configure > My Proxy > Basic** page and disable Data Security.

   When the upgrade is complete, return to the **Configure > My Proxy > Basic** page, enable Data Security, and restart Content Gateway. Then, navigate to the **Configure > Security > Data Security** page and confirm that automatic registration was successful. If it was not, manually register with Data Security.
2. Log on to the Content Gateway Linux host and acquire root permissions:

   ```
   su root
   ```
3. Disable any currently running firewall on this machine for the duration of the upgrade. Bring the firewall back up after the upgrade is complete, opening ports used by Content Gateway.

   For example, if you are running IPTables:

   a. At a command prompt, enter **service iptables status** to determine if the firewall is running.

   b. If the firewall is running, enter **service iptables stop**.

c. After upgrade, restart the firewall. In the firewall, be sure to open the ports used by Content Gateway on this machine. See Websense TRITON Enterprise default ports for more information.

4. Download the Content Gateway version 7.8.x installer from mywebsense.com and save it to a temporary directory. For example, place it in:

   ```
   /tmp/wcg_v78
   ```

5. Unpack the Content Gateway installer tar archive:

   ```
   cd /tmp/wcg_v78
   tar -xvzf <installer tar archive>
   ```

   Important

   If SELinux is enabled, set it to permissive, or disable it before installing Content Gateway. Do not install or run Content Gateway with SELinux enabled.

6. If you intend to upgrade Red Hat Enterprise Linux 6.x to a more recent version, perform the upgrade now. See your Red Hat Enterprise Linux documentation.

7. In the directory where you unpacked the tar archive (for example, /tmp/wcg_78), start the installation/upgrade script.

   ```
   ./wcg_install.sh
   ```

   Respond to the prompts.

   Content Gateway is installed and runs as **root**.

   Note

   Up to the point that you are prompted to confirm your intent to upgrade, you can quit the installer by pressing CTRL+C. If you change your mind after you choose to continue, do **not** use CTRL+C to stop the process. Instead, allow the installation to complete and then uninstall.

8. If your server does not meet the minimum hardware requirements or is missing required operating system packages, you will receive error or warning messages. For example:

   ```
   Error: Websense Content Gateway v7.8.x on x86_64 requires
   several packages that are not present on your system.
   Please install the following packages: <list of packages>
   If you are connected to a yum repository you can install
   these packages with the following command:
   yum install <list of packages>
   See the Websense Technical Library (www.websense.com/
   library) for information about the software requirements
   for x86_64 installation.
   ```

   You may run into this error because 32-bit packages were required for v7.7.x and 64-bit libraries are required for v7.8.x.

To make it easier to install the needed packages, the Content Gateway distribution includes a Linux "rpm" containing the needed packages. To install its contents, ensure that the operating system has access to the Red Hat Linux distribution library (for example the DVD), and enter:

```
yum install wcg_deps-1-0.noarch.rpm
```

Upon successful completion, a list of updated packages is displayed and then the word "Complete!".

Here is an example of a system resource warning:

```
Warning: Websense Content Gateway requires at least 6
gigabytes of RAM.

Do you wish to continue [y/n]?
```

Enter **n** to end the installation and return to the system prompt.

Enter **y** to continue the upgrade. You should not install or upgrade on a system that does not meet the minimum requirements. If you choose to run Content Gateway after receiving a system resource warning, performance and stability may be affected.

9. Read the subscription agreement. At the prompt, enter **y** to accept the agreement and continue the upgrade, or **n** to cancel.

   ```
   Do you accept the above agreement [y/n]? y
   ```

10. The installer checks for the presence of an existing Content Gateway installation. When asked, choose to replace the existing version with version 7.8.x.

    ```
    WCG version 7.7.n-nnnn was found.

    Do you want to replace it with version 7.8.x-nnnn [y/n]? y
    ```

11. Existing settings and logs are copied to backup files and stored. For example:

    ```
    Stopping Websense Content Gateway processes...done

    Copying settings from /opt/WCG to /root/WCG/OldVersions/
    7.7.0-1418-PreUpgrade/...done

    Zipping configuration archive...done

    Moving log files from /opt/WCG/logs to /opt/WCG_tmp/logs/
    ...done
    ```

12. You can either re-use the installation selections you entered during the last install, or provide new answers to all installation prompts, such as admin password, admin email address, Policy Server IP address, etc.:

    ```
    Previous installation selections </root/WCG/Current/
    WCGinstall.cfg> found.

    Use previous installation selections [y/n]?
    ```

    Enter **y** to use previous installation selections.

    Enter **n** to revert to Websense default values, and receive all installation questions and answer them again.

13. If you answered **y** at Step 11, then you can also leave proxy settings at their current values or revert to Websense default values (which perform a fresh install!).

    ```
    Restore settings after install [y/n]?
    ```

Enter **y** to keep the proxy settings as they are.

Enter **n** to restore Websense default settings for the proxy.

Caution: If you answer **n** (no), the current installation of Content Gateway is removed, and a fresh install of 7.8.x begins. See Installing Websense Content Gateway for a detailed description of the installation procedure. This is not an upgrade, but rather a fresh install.

14. The previously installed version of Websense Content Gateway is removed, and the settings and selections you chose to retain are re-used. Details of the upgrade process are output to the screen. Please wait.

```
*COMPLETED* Websense Content Gateway 7.8.x-nnnn
installation.

A log file of this installation process has been written to
/root/WCG/Current/WCGinstall.log

For full operating information, see the Websense Content
Gateway Help system.

Follow these steps to start the Websense Content Gateway
management interface (Content Gateway Manager):

-------------------------------------------------------------

1. Start a browser.

2. Enter the IP address of the Websense Content Gateway
server, followed by a colon and the management interface
port (8081 for this installation). For example: https://
11.222.33.44:8081.

3. Log on using username admin and the password you chose
earlier.

A copy of the CA public key used by the Manager is located in
/root/WCG/.
```

15. The automated portion of the upgrade is now complete, and the proxy software is running.

    If you chose to revert to Websense default proxy settings, be sure to configure any custom options.

16. Check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

    All services should be running. These include:

    - Content Cop
    - Websense Content Gateway
    - Content Gateway Manager

- Analytics Server

Important

If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for:

```
/opt/WCG/config/internal/no_cop
```

If the file exists, remove it and start Content Gateway:

```
/opt/WCG/WCGAdmin start
```

To finish the upgrade, be sure to perform the post-upgrade instructions at the end of this document.

Content Gateway: Upgrade Red Hat Enterprise Linux 5-series to 6-series during the Content Gateway upgrade

Content Gateway versions 7.7.x run on Red Hat Enterprise Linux 5-series and 6-series.

Content Gateway version 7.8.x runs on 64-bit, Red Hat Enterprise Linux 6-series only.

Use the following procedure to upgrade the host operating system while upgrading Content Gateway. Read it completely before beginning the process.

Important

If you want to retain the existing Content Gateway log files (in **/opt/WCG/logs**), determine their total size, identify a location on your network that has enough space to hold the files, and copy them there.

When the upgrade is complete, copy the files back to /opt/WCG/logs and delete the files from the temporary location.

1. Log on to the Content Gateway v7.7.x host and acquire **root** privileges. All steps must be performed as root.
2. Obtain the Content Gateway v7.8.x gzip installation file, place it on the v7.7.x machine, and use the v7.8.x **wcg_config_utility.sh** script and **configFiles.txt** support file to backup your system.
   a. Download the Content Gateway v7.8.x installer from mywebsense.com. Save it in a convenient location on the network; you'll need it again later. Place a copy in a temporary directory on your Content Gateway server (the Red Hat Enterprise Linux 5-series system). For example, place it in:

      ```
      /tmp/wcg_v78
      ```

   b. Unpack the installer gzip archive:

      ```
      cd /tmp/wcg_v78
      ```

```
tar -xvzf <installer gzip tar archive>
```

c. In /tmp/wcg_v78 unpack **lx86inst.tar**:

```
tar -xvf lx86inst.tar
```

This tar command does not use the 'z' flag because the tar file is not a gzip.

d. Change directory to scripts:

```
cd ./scripts/
```

e. Using **wcg_config_utility.sh** create a backup of Content Gateway v7.7.x and save it to a trusted location on the network:

```
./wcg_config_utililty.sh create WCGbackup
```

This creates **WCGbackup.tar.gz** in the current directory.

3. Copy **WCGbackup.tar.gz** to a reliable location on the network where it can easily be retrieved after the operating system upgrade.
4. If you are upgrading Red Hat Enterprise Linux on this machine, uninstall Content Gateway. See Uninstalling Content Gateway and continue with Step 6.
5. If you want to keep the current machine as a fallback option, power down the computer and disconnect it from the network.

> **Note**
>
> You can only revert to the original machine if the other Web Security components are also reverted to the matching (original) 7.7.x version. When that is the case, you can simply reconnect the Content Gateway host machine to the network and power up. Content Gateway v7.7.x will re-register with Web Security.
>
> If you want to repurpose the machine, do not reconnect it to the network until after you have uninstalled Content Gateway and assigned the machine a new IP address and hostname.

6. Applying the same hostname, ethernet interface, and IP address used with Red Hat Enterprise Linux 5, install Red Hat Enterprise Linux 6. Updates 6.4 and 6.5 are certified with v7.8.x. Updates 6.0, 6.1, 6.2, and 6.3 are supported.

> **Note**
>
> Content Gateway is designed to run on Red Hat Enterprise Linux, **Basic Server** package. This is the default installation configuration and must be confirmed.
>
> For information on installing Red Hat Enterprise Linux 6, see Red Hat Enterprise Linux 6 Installation Guide.
>
> For a list of required libraries, see Required libraries in Red Hat Enterprise Linux 6.

7. In the directory where you downloaded the **WebsenseCG78Setup_Lnx.tar.gz** tar archive, begin the installation, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

   The installer installs Content Gateway in /opt/WCG. It is installed as **root**.

   > **Note**
   >
   > Up to the configuration summary, you can quit the installer by pressing CTRL-C. If you choose to continue the installation past the configuration summary and you want to quit, do **not** use CTRL-C. Instead, allow the installation to complete and then uninstall it.
   >
   > If you want to change your answer to any of the installer prompts, you will be given a chance to start over at the first prompt once you reach the configuration summary; you do not have to quit the installer.

8. If your system does not meet the minimum recommended requirements, you receive a warning. For example:

   ```
   Warning: Websense Content Gateway requires at least 4
   gigabytes of RAM.
   Do you wish to continue [y/n]?
   ```

   Enter **n** to end the installation, and return to the system prompt.

   Enter **y** to continue the installation. If you choose to run Content Gateway after receiving this warning, performance may be affected.

9. Read the subscription agreement. At the prompt, enter **y** to continue installation or **n** to cancel installation.

   ```
   Do you accept the above agreement [y/n]? y
   ```

10. Enter and confirm a password for the Content Gateway Manager administrator account:

    ```
    Enter the administrator password for the Websense Content
    Gateway management interface.
    Username: admin
    Password:> (note: cursor will not move as you type)
    Confirm password:>
    ```

    This account enables you to log on to the management interface for Content Gateway, known as Content Gateway Manager. The default username is **admin**.

To create a strong password (recommended), use 8 or more characters, with at least 1 each of the following: capital letter, lower case letter, number, special character.

Important

The password length must be 16 characters or less. Also, it cannot contain the following characters:

- space
- $ (dollar symbol)
- : (colon)
- ` (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- " (double-quote)

Note

As you type a password, it may seem that nothing is happening—the cursor will not move nor will masked characters be shown—but the characters are being accepted. After typing a password, press **Enter**. Then repeat to confirm it.

11. Enter an email address where Content Gateway can send alarm messages:

    ```
    Websense Content Gateway requires an email address for
    alarm notification.

    Enter an email address using @ notation: [] >
    ```

    Be sure to use @ notation (for example, user@example.com). Do not enter more than 64 characters for this address.

12. Enter the IP address for Policy Server:

    ```
    Enter the Policy Server IP address (leave blank if
    integrating with Data Security only): [] >
    ```

    Use dot notation (i.e., xxx.xxx.xxx.xxx). The address must be IPv4.

13. Enter the IP address for Filtering Service:

    ```
    Enter the Filtering Service IP address: [<Policy Server
    address>] >
    ```

    The default is the same address as Policy Server.

14. Review default Content Gateway ports:

    ```
    Websense Content Gateway uses 11 ports on your server:

    -------------------------------------------
    '1'  Websense Content Gateway Proxy Port  8080
    '2'  Web Interface port                   8081
    '3'  Auto config port                     8083
    ```

```
'4'  Process manager port                8084
'5'  Logging server port                 8085
'6'  Clustering port                     8086
'7'  Reliable service port               8087
'8'  Multicast port                      8088
'9'  HTTPS inbound port                  8070
'N'  HTTPS outbound port                 8090
'M'  HTTPS management port               8071

Enter the port assignment you would like to change:

'1-9,N,M,D' - specific port changes
'X'  - no change
'H'  - help
[X] >
```

Change a port assignment if it will conflict with another application or process on the machine. Otherwise, leave the default assignments in place. Any new port numbers you assign must be between 1025 and 65535, inclusive.

15. For clustering, at least two network interfaces are required. If your machine has only one, the following prompt appears:

    ```
    Websense Content Gateway requires at least 2 interfaces
    to support clustering. Only one active network interface
    is detected on this system.
    ```

    Press **Enter** to continue installation and skip to Step 14.

16. If two or more network interfaces are found on this machine, you are asked whether this instance of Content Gateway should be part of a cluster:

    ```
    Websense Content Gateway Clustering Information

    ------------------------------------------------

    '1' - Select '1' to configure Websense Content Gateway
            for management clustering. The nodes in the cluster
            will share configuration/management information
            automatically.

    '2' - Select '2' to operate this Websense Content Gateway
            as a single node.


    Enter the cluster type for this Websense Content Gateway
    installation:

    [2] >
    ```

    If you do not want this instance of Content Gateway to be part of a cluster, enter 2.

    If you select 1, provide information about the cluster:

    ```
    Enter the name of this Websense Content Gateway cluster.

    ><cluster_name>
    ```

    Note: All members of a cluster must use the same cluster name.

    ```
    Enter a network interface for cluster communication.

    Available interfaces:
    <interface, e.g., eth0>
    <interface, e.g., eth1>
    ```

```
Enter the cluster network interface:
>
Enter a multicast group address for cluster <cluster_name>.
Address must be between 224.0.1.27 - 224.0.1.254:
[<default IP address>] >
```

17. For Content Gateway to act as a web cache, a raw disk must be present on this machine. If no raw disk is detected, the following prompt appears:

    ```
    No disks are detected for cache.
    Websense Content Gateway will operate in PROXY_ONLY mode.
    ```

    Content Gateway will operate as a proxy only and will not cache Web pages. Press ENTER to continue the installation and skip to Step 16.

18. If a raw disk is detected, you can enable the web cache feature of Content Gateway:

    > **Note**
    > If you choose to not enable raw disk cache now, cache disks may be added after Content Gateway has been installed. For instructions, see Content Gateway Manager Help.

    ```
    Would you like to enable raw disk cache [y/n]? y
    ```

    a. Select available disks from the list. Selected disks become dedicated cache disks and cannot be used for any other purpose. Cache disks must be raw. Aggregate disk cache size should not exceed 147 GB.

    ```
    Select available disk resources to use for the cache.
    Remember that space used for the cache cannot be used for
    any other purpose.
    Here are the available drives
    (1) /dev/sdb 146778685440 0x0
    ```

    Note: The above drive is only an example.

    > **Warning**
    > Although it might be listed as available, do **not** use an LVM (Logical Volume Manager) volume as a cache disk.

    b. Indicate if you want to add or remove disks individually or as a group.

    ```
    Choose one of the following options:
    'A'   - Add disk(s) to cache
    'R'   - Remove disk(s) from cache
    'S'   - Add all available disks to cache
    'U'   - Remove all disks from cache
    'X'   - Done with selection, continue Websense
            Content Gateway installation.
    ```

```
Option: > A
[ ] (1) /dev/sdb 146778685440 0x0
```

c. Specify which disk or disks to use for the cache.

```
Enter number to add item, press 'F' when finished:
[F] >1
Item '1' is selected
[F] >
```

d. Your selections are confirmed. Note the "x" before the name of the disk.

```
Here is the current selection
[X] (1) /dev/sdb 146778685440 0x0
```

e. Continue based on your choice in Step b, pressing **X** when you have finished configuring cache disks.

```
Choose one of the following options:
'A'   - Add disk(s) to cache
'R'   - Remove disk(s) from cache
'S'   - Add all available disks to cache
'U'   - Remove all disks from cache
'X'   - Done with selection, continue Websense
        Content Gateway installation.
Option: >X
```

19. You can elect to send Websense, Inc., information about scanned content (Note: individual users are never identified):

```
Websense Content Gateway has the ability to send usage
statistics, information about scanned content and activated
product features to Websense Inc. for the purpose of
improving the accuracy of scanning, filtering and
categorization.
Would you like to allow this communication with Websense,
Inc. ? [y/n]
```

20. A configuration summary appears, showing your answers to the installer prompts (note: summary below is an example):

```
Configuration Summary
---------------------------------------------------------
Websense Content Gateway Install Directory : /opt/WCG
Admin Username for Content Gateway Manager: admin
Alarm Email Address                        : <email address>
Policy Server IP Address                   : <IP address>
Filtering Service IP Address               : <IP address>
Websense Content Gateway Cluster Type      : NO_CLUSTER
Websense Content Gateway Cache Type        : LRAW_DISK
  Cache Disk                               : /dev/sdb
  Total Cache Partition Used               : 1
                  ******************
                  *  W A R N I N G  *
```

```
                    ********************
    CACHE DISKS LISTED ABOVE WILL BE CLEARED DURING
    INSTALLATION!! CONTENTS OF THESE DISKS WILL BE
    COMPLETELY LOST WITH NO CHANCE OF RETRIEVAL.

    Installer CANNOT detect all potential disk mirroring
    systems. Please make sure the cache disks listed
    above are not in use as mirrors of active file
    systems and do not contain any useful data.

Do you want to continue installation with this configuration
[y/n]?
```

If you want to make changes, enter **n** to restart the installation process at the first prompt. To continue and install Content Gateway configured as shown, enter **y**.

Important

If you enter **y** to proceed but you decide you want to cancel the installation, do not attempt to quit the installer by pressing CTRL-C. Allow the installation to complete. Then uninstall it.

21. Wait for the installation to complete.

    Note the location of the certificate required for Content Gateway Manager: **/root/WCG/content_gateway_ca.cer**. See the Getting Started section of the Content Gateway Manager Help for information on importing this certificate.

Note

The subscription key is shared automatically with Content Gateway if it has already been specified in the Web Security manager.

If you receive an email from Content Gateway (to the address you specified during installation) with "WCG license download failed" in the subject line, this alert does not mean a problem occurred with the installation. The alert indicates that your deployment may require you to manually enter the subscription key in Content Gateway Manager.

See the Getting Started section of the Content Gateway Manager Help for information on entering your subscription key.

22. When installation is complete, reboot the Content Gateway server.
23. When the reboot is complete, check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

    All services should be running. These include Content Cop, Websense Content Gateway, Content Gateway Manager, and Analytics Server.
24. Copy the **WCGbackup.tar.gz** file, saved in step 3, to:

```
~/WCG/Current/
```

25. Restore the configuration archive. As root:

    ```
    cd ~/WCG/Current/
    ./wcg_config_utility.sh restore WCGbackup.tar.gz
    ```

26. Check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

    All services should be running. These include:

    - Content Cop
    - Websense Content Gateway
    - Content Gateway Manager
    - Analytics Server

> **Important**
> If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for:
>
> ```
> /opt/WCG/config/internal/no_cop
> ```
>
> If the file exists, remove it and start Content Gateway:
>
> ```
> /opt/WCG/WCGAdmin start
> ```

To finish the upgrade, be sure to perform the steps at the end of this document.

Step 11: Upgrade any additional components

Upgrade any additional server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines.

See:

- *Additional components: Windows upgrade instructions*, page 39
- *Additional components: Linux upgrade instructions*, page 40

Additional components: Windows upgrade instructions

1. Log on to the installation machine with an account having **domain** and **local** administrator privileges.
2. Close all applications and stop any antivirus software.

> **Warning**
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

3. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON78xSetup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
4. Right-click **WebsenseTRITON78xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
5. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
6. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
7. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
8. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
9. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

   Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
10. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
11. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

12. If you stopped your antivirus software, restart it.

Additional components: Linux upgrade instructions

1. Log on the installation machine with administrator privileges (typically, as **root**).
2. Close all applications and stop any antivirus software.
3. Check the **etc/hosts** file. If there is no host name for the machine, add one.
4. Create a setup directory for the installer files, such as **/root/Websense_setup**.

5. Download the Web Security Linux installer from the Downloads page at mywebsense.com. The installer file is called **WebsenseWeb78xSetup_Lnx.tar.gz**.
6. Uncompress the installer file and use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

   To launch the command-line installer, omit the -g switch:

   ```
   ./install.sh
   ```
7. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

8. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
9. On the Websense Upgrade screen, select **Start the upgrade** and then click **Next**.
10. When you click **Next**, a "Stopping All Services" progress message appears. Wait for Websense services to be stopped.

    The Pre-Upgrade Summary screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually using the **/opt/Websense/WebsenseAdmin stop** command. You can leave the installer running when you do so. Once you have manually stopped the services, return to the installer.
11. On the Pre-Upgrade Summary screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
12. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
13. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

14. If you stopped your antivirus software, restart it.

Step 12: Post-upgrade activities for Content Gateway

After you have finished upgrading components, perform the following steps to ensure that your Content Gateway upgrade is complete.

1. If at the start of the upgrade process you manually moved your existing log files to a temporary location, move them back to **/opt/WCG/logs** and delete the files in the temporary location.
2. Register Content Gateway nodes in the Web Security manager on the **Settings > Content Gateway Access** page. Registered nodes add a link to the Content Gateway Manager logon portal and provide a visual system health indicator: a green check mark or a red X.
3. Configure Content Gateway system alerts in the Web Security manager. A subset of Content Gateway system alerts are sent to the Web Security manager (in addition to Content Gateway Manager). To configure which alerts are sent, in the Web Security manager go to the **Settings > Alerts > System** page.
4. If you use SSL support:
   a. If your clients don't yet use a SHA-1 internal Root CA, create and import a SHA-1 Root CA into all affected clients. See Internal Root CA in Content Gateway Help.
   b. Using the notes you compiled prior to upgrade, rebuild your Static Incident list.
   c. Using the notes you compiled prior to upgrade, recreate your customized error message pages. (Not required for upgrades from 7.8.x.)
5. If you use proxy user authentication, review the settings on the **Global Authentication Options** page (**Configure > Security > Access Control > Global Configuration Options**).
6. If you use IWA user authentication, confirm that the AD domain is still joined. Go to **Monitor > Security > Integrated Windows Authentication**. If it is not joined, rejoin the domain. Go to **Configure > Security > Access Control > Integrated Windows Authentication**.
7. If you use Multiple Realm Authentication rules, review the converted Rule-Based Authentication configuration. Go to **Configure > Security > Access Control**.
   a. Check the **Domains** page.
      - IWA domains that were joined before upgrade should still be joined. Select each domain, click **Edit** and give each domain a unique **Domain Identifier**.
      - LDAP and Legacy NTLM domains should be listed. Select each domain, click **Edit** and give each domain a unique domain identifier.
   b. Check each rule.
      - Go to the **Authentication Rules** page and enter the editor.
      - Select each rule and check the configuration.

- For Multiple Realm Authentication rules that used Cookie Mode Caching, the Source IP address list will have been copied to the cookie list on the Global Authentication Option page.
- Check that the expected domain is in the **Auth Sequence** list.

Important: The Rule-Based Authentication feature is very rich and can satisfy many user authentication requirements. To make best use of it, please read Rule-Based Authentication.

8. If you use IWA with a load balancer in v7.7.3 (a custom configuration):
   - IWA with a load balancer is not supported in v7.8.1.
   - IWA with a load balancer is supported in v7.8.2 and v7.8.3. To get the support, upgrade to v7.8.1 and then to v7.8.2 or v7.8.3. Follow the special configuration steps described in the v7.8.2 Release Notes or the v7.8.3 Release Notes.
9. If Web Security Gateway Anywhere and Data Security are deployed together, confirm that Content Gateway has automatically re-registered with Data Security Management Server. If it has not, manually re-register.
   a. Ensure that the Content Gateway and Data Security Management Server system clocks are synchronized to within a few minutes.
   b. In the Content Gateway manager:
      - Go to **Configure > My Proxy > Basic**, ensure that **Data Security: Integrated on-box** is enabled, and click **Apply**.
      - Next to **Integrated on-box**, click the **Not registered** link. This opens the **Configure > Security > Data Security registration** screen.
      - Enter the IP address of the Data Security Management Server.
      - Enter a user name and password for logging onto the Data Security manager. The user must be a Data Security administrator with Deploy Settings privileges.
      - Click **Register**. If registration is successful, a message confirms the result and prompts you to restart Content Gateway. If registration fails, an error message indicates the cause of failure. Correct the problem and perform the registration process again.
10. If Web Security Gateway Anywhere and Data Security are deployed together and upgraded from v7.7.x to version 7.8.x, you must remove stale entries of Content Gateway instances registered in Data Security system modules:
    a. Log onto the TRITON console.
    b. Select the **Data Security** tab.
    c. Select **Settings > Deployment > System Modules**.
    d. Listed are 2 instances of each Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.
    e. Click **Deploy**.
11. If Web Security Gateway Anywhere and Data Security are deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance must be deleted

from the list of Data Security system modules or the deployment will fail. Go to the **Data Security** > **Settings** > **Deployment** > **System Modules** page, click on the affected Content Gateway instance to open its **Details** page, click **Delete** and then **Deploy**.